In the Claims:

Please amend the claims as follows:

1 (Currently amended). In an information stream associated with deliverable published software from a software publisher to a customer, an arrangement for software protection comprising a personalization, said personalization incorporated into the information stream by the software publisher prior to delivery of the published software to the customer and prior to receipt of the published software by the customer, and containing pre-existing personal information fundamentally related to the customer.

2 (Original). The arrangement as in claim 1, wherein the deliverable published software is intended to execute on a plurality of computers, and wherein said personalization is not fundamentally related to any specific computer of the plurality.

3 (Original). The arrangement as in claim 1, wherein the deliverable published software is intended to execute on a plurality of computers, each of the plurality of computers having a configuration, and wherein said personalization is not fundamentally related to any specific configuration.

4 (Original). The arrangement as in claim 1, wherein the deliverable published software is intended to execute on computers belonging to a class of computer, and wherein the deliverable published software executes in substantially identical functional form on substantially all computers of the class of computer.

5 (Currently amended). The arrangement as in claim 1, wherein said personalization is not associated with, and does not activate, any usage restriction on the deliverable published software.

6 (Original). The arrangement as in claim 1, wherein said personalization does not have a fixed address within the information stream.

7 (Original). The arrangement as in claim 1, wherein said personalization does not have a fixed extent within the information stream.

8 (Original). The arrangement as in claim 1, wherein said personalization is authenticated.

9 (Original). The arrangement as in claim 8, wherein said personalization is in an encrypted form within the information stream.

10 (Canceled).

11 (Original). The arrangement as in claim 1, wherein the information stream contains at least one executable module, and wherein said personalization is contained within said at least one executable module.

12 (Original). The arrangement as in claim 1, further comprising a personalization validation module operative to validating a personalization.

13 (Currently amended). The arrangement as in claim 12, wherein said personalization ~~verification~~ validation module is further operative to validating an output file.

14 (Currently amended). The arrangement as in claim 12, wherein the information stream contains at least one executable module, and wherein said personalization ~~verification~~ validation module is further operative to validating said at least one executable module.

15 (Original). The arrangement as in claim 12, wherein said personalization validation module is further operative, upon not detecting a valid personalization, to initiate an action included in the group containing:

(a) program termination;

(b) operating the software in a demonstration mode; and

(c) operating the software in a restricted mode.

16 (Currently amended). The arrangement as in claim 1, wherein the information stream contains at least one executable module having an ~~authentication~~ authenticated personalization, and wherein said executable module executes in a secure computer environment operative to validating said ~~authentication~~ authenticated personalization.

17 (Original). The arrangement as in claim 1, wherein at least part of the deliverable published software is written in the Java language.

18 (Original). The arrangement as in claim 17, wherein at least part of the deliverable published software is contained in a Java archive.

19 (Original). The arrangement as in claim 18, wherein said Java archive is signed with an archive signature.

20. (Original) The arrangement as in claim 16, wherein said secure computer environment is operative to executing Java software.

21 (Original). The arrangement as in claim 12, wherein said personalization is in an encrypted form within the information stream, and wherein said personalization validation module is further operative to decrypting said encrypted form.

22 (Original). The arrangement as in claim 21, wherein said encrypted form is according to a public key cryptosystem having a public key, and wherein said personalization validation module has access to said public key.

23 (Currently amended). The arrangement as in claim 1, wherein the information stream contains at least one executable module operative to writing an output file containing information derived from said personalization, and wherein said information derived from said personalization in said output file is operative to being separately validated.

24 (Currently amended). A method for protecting published software ordered by a customer, the method comprising ~~the steps of~~:

(a) obtaining pre-existing personal information fundamentally related to the customer;

(b) producing a personal information module~~,~~ from said pre-existing personal information fundamentally related to the customer~~, a personal information module~~; and

(c) producing an executable module deriving at least in part from said personal information module and incorporating at least part of said pre-existing personal information fundamentally related to the customer;

wherein at least one of said producing a personal information module and said producing an executable module is performed prior to delivery of the published software to the customer and prior to receipt of the published software by the customer.

25 (Currently amended). The method as in claim 24, further comprising ~~the steps of~~:

(d) authenticating said personal information module; and

(e) providing a personalization validation module, from which derives at least in part from said executable module.

26 (Currently amended). The method as in claim 24, further comprising ~~the steps of~~:

(d) incorporating said executable module within a Java archive; and

(e) authenticating said Java archive with an archive signature.

27 (Currently amended). The method as in claim 25, further comprising ~~the steps of~~:

(f) incorporating said executable module within a Java archive; and

(g) authenticating said Java archive with an archive signature.

28 (Currently amended). A system for protecting published software ordered by a customer, the system comprising:

(a) a personal information collector for collecting pre-existing personal information fundamentally related to the customer, wherein said personal information collector collects personal information remotely from the customer via a communications channel;

(b) a personalization compiler, for producing, from said pre-existing personal information fundamentally related to the customer, a personalization module; and

(c) an executable module builder, for producing deliverable published software containing said pre-existing personal information fundamentally related to the customer and derived at least in part from said personalization module.

29 (New). The system as in claim 28, wherein said communications channel is a network.

30 (New). The system as in claim 29, wherein said network is the Internet.

31 (New). The arrangement as in claim 1, wherein at least part of said personalization is operative to being displayed on a computer without requiring customer input of said at least part of said personalization.

32 (New). The arrangement as in claim 31, wherein said being displayed on a computer comprises being displayed in a display location selected from the group consisting of: title bar, window banner, splash window, help window, about window, main window, installation window, notification window, file listing window, and interactive window.

33 (New). The arrangement as in claim 31, wherein the information stream contains at least one executable module operative to displaying said at least part of said personalization.